Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: May 20, 2024	**Entry:** 1
Description	Incident occurring on Tuesday at 9 AM Business operations severely disrupted due to ransomware - phishing email with a malicious attachment downloaded ransomware note onto computers Ransom note stated that the company's files were encrypted and demanded money in exchange for the decryption key
Tool(s) used	

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ Unethical hackers that target medical and transportation businesses
	• **What** happened?
	  ○ An employee opened a malicious email attached from a phishing email that allowed the ransomware to be downloaded onto the system. This allowed the hackers to access to the company's network and encrypt the files
	• **When** did the incident occur?

	○ Tuesday at 9 AM ● **Where** did the incident happen? ○ Company's address ● **Why** did the incident happen? ○ Hacker group deployed ransomware for financial gain
Additional notes	How do we reinstate access to the files without giving up money? How could the healthcare company prevent an incident like this from occurring again?

Date: May 28, 2024	**Entry: 2**
Description	You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Malicious attacker**

	• **An employee downloaded a file that was sent to them in an email. The file had malicious payload on it that was executed upon download.**
	• When did this occur:
	  ○ 1:11 p.m.: An employee receives an email containing a file attachment.
	  ○ 1:13 p.m.: The employee successfully downloads and opens the file.
	  ○ 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.
	  ○ 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.
	• **Where** - Employee's place of work
	• **Why** - Employee opened a malicious file

Additional notes	

Date: 2024-05-30	**Entry: 3**
Description	Received a phishing alert about a suspicious file being downloaded on an employee's computer.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who**: Employee

	• **What**: Employee received an email stating that a person was interested in a job posting and was asked to open and download the attached resume. • **When**: Wednesday, July 20, 2022 09:30:14 AM • **Where**: Employee's business office • **Why**: Employee downloaded the resume which had a trojan embedded into it.
Additional notes	Training to employee on how to identify phishing emails and best practices when faced with one.

Date: 2024-06-11	**Entry: 4**
Description	Use WireShark to inspect packet data and apply filters to sort through pack information efficiently.
Tool(s) used	WireShark
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	